Beispiel Diffie-Hellmann-Verfahren

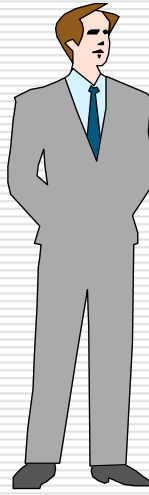
leicht vereinfacht ...

Alice

Hallo Bob,
wir müssen
reden.
Ungestört!

Hallo Alice,
wir müssen
reden.
Ungestört!

Bob



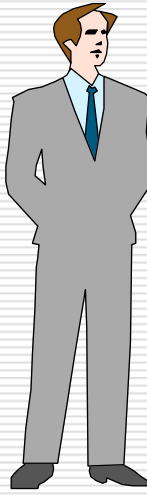
Hihi, wird
nichts ...

Melroy

Alice

erst brauchen wir eine große Primzahl.

Bob



Nützt euch nichts ...

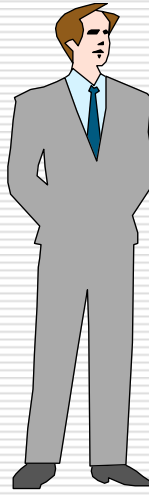
Melroy

Alice

n=13

Nehmen wir die 13.

Bob



n=13

Jetzt kenne ich schon die Zahl **n**!

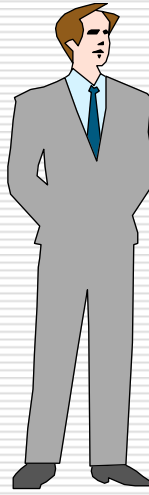
Melroy

n=13

Alice

Oh, die ist wirklich groß ...

Bob



n=13

n=13

Jetzt kenne ich schon die Zahl **n**!

Melroy

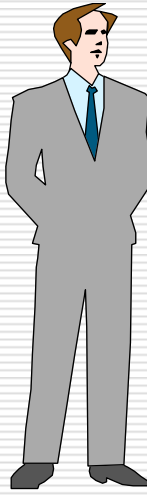
n=13

Alice

n=13

Dann brauchen wir noch eine Zufallszahl.

Bob



n=13

Nützt euch nichts ...

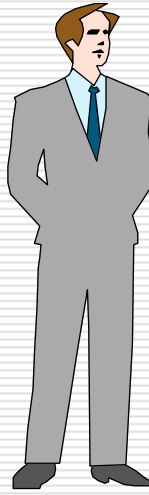
Melroy

n=13

Alice

Ganz zufällig bin ich auf die 6 gekommen.

Bob



n=13
g=6

Jetzt habe ich auch noch **g**!

Melroy

n=13
g=6

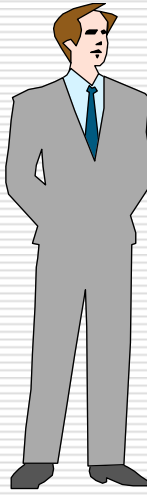
n=13
g=6

Alice

n=13
g=6

Super!

Bob



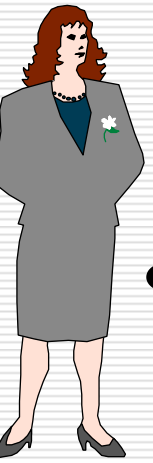
n=13
g=6

Nützt euch nichts ...

Melroy

n=13
g=6

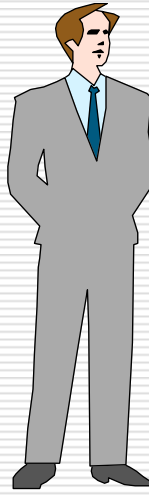
Alice



meine geheime Zufallszahl: x=5

meine geheime Zufallszahl: y=7

Bob



n=13
g=6
x=5

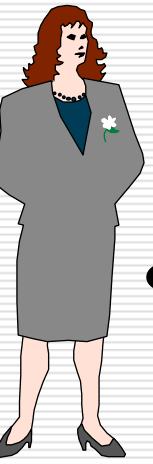
was machen die da jetzt nur?

Melroy

n=13
g=6

n=13
g=6
y=7

Alice

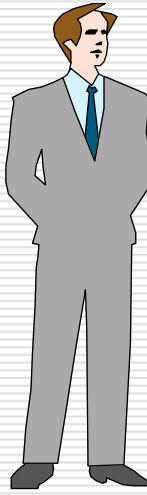


Jetzt berechne ich meine öffentliche Zahl:

n=13
g=6
x=5

Jetzt berechne ich meine öffentliche Zahl:

Bob



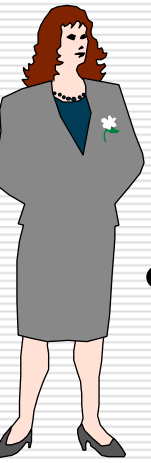
n=13
g=6
y=7

was machen die da jetzt nur?

Melroy

n=13
g=6

Alice

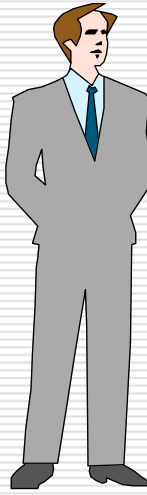


X=g^x mod n

n=13
g=6
x=5

Y=g^y mod n

Bob



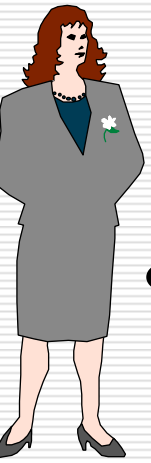
n=13
g=6
y=7

was machen die da jetzt nur?

Melroy

n=13
g=6

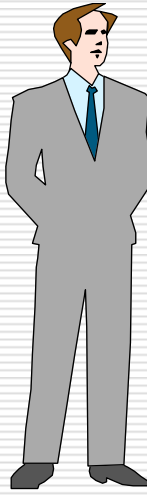
Alice



X=2

Y=7

Bob



n=13
g=6
x=5
X=2

was machen die da jetzt nur?

Melroy

n=13
g=6

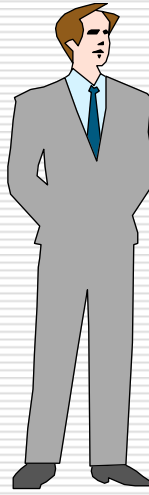
n=13
g=6
y=7
Y=7

Alice

Bob,
meine
öffentliche Zahl
ist 2.

Alice,
meine
öffentliche Zahl
ist 7.

Bob



n=13
g=6
x=5
X=2
Y=7

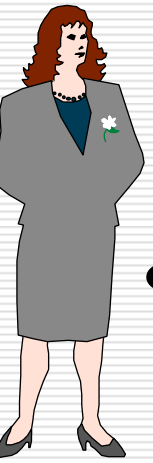
Hihi,
wieder zwei
neue Werte!

Melroy

n=13
g=6
X=2
Y=7

n=13
g=6
y=7
Y=7
X=2

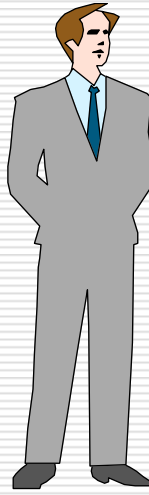
Alice



Jetzt berechne ich den geheimen Schlüssel

Jetzt berechne ich den geheimen Schlüssel

Bob



n=13
g=6
x=5
X=2
Y=7

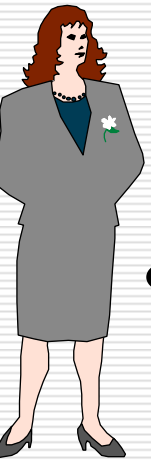
was machen die da jetzt nur?

Melroy

n=13
g=6
X=2
Y=7

n=13
g=6
y=7
Y=7
X=2

Alice

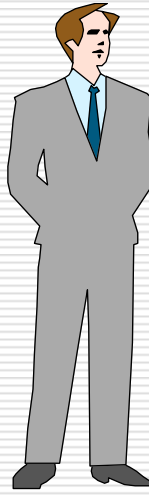


k=Y^x mod n

n=13
g=6
x=5
X=2
Y=7

k=X^y mod n

Bob



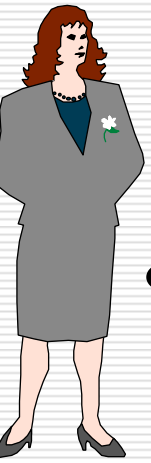
n=13
g=6
y=7
Y=7
X=2

was machen die da jetzt nur?

Melroy

n=13
g=6
X=2
Y=7

Alice

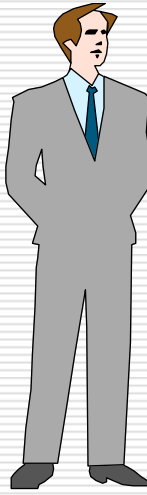


Der geheime Schlüssel ist **11**

n=13
g=6
x=5
X=2
Y=7
k=11

Der geheime Schlüssel ist **11**

Bob



n=13
g=6
y=7
Y=7
X=2
k=11

was machen die da jetzt nur?

Melroy

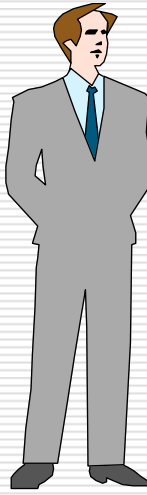
n=13
g=6
X=2
Y=7

Alice

Jetzt belauscht uns keiner mehr!

Jetzt belauscht uns keiner mehr!

Bob



k=11

k=11

STOP!!!
Ich kann **k** noch nicht berechnen!!!

Melroy

n=13
g=6
X=2
Y=7